Gloucestershire Hospitals NHS

NHS Foundation Trust

TRUST POLICY

In the case of hard copies of this policy the content can only be assured to be accurate on the date of issue marked on the document.

The Policy framework requires that the policy is fully reviewed on the date shown, but it is also possible that significant changes may have occurred in the meantime.

The most up to date policy will always be available on the Intranet Policy web site and staffs are reminded that assurance that the most up to date policy is being used can only achieved by reference to the Policy web site.

IT SECURITY POLICY
By
IT Service Department

This document may be made available to the public and persons outside of the Trust as part of the Trust's compliance with the Freedom of Information Act 2000

Date of Issue…November 2006……. Review Date… November 2007…….

Gloucestershire Hospitals NHS

NHS Foundation Trust

TRUST POLICIES

Authorisation Form

DOCUMENT:
I.T. SECURITY POLICY

We the author/sponsor confirm that this policy does not involve or impact on any of the following;

(Please place an X in a, b and c, or in 2, if this applies)

1**a** Eliminating racial discrimination ☐
1**b** Promoting equality of opportunity ☐
1**c** promoting good race relations ☐
or where it does impact

2. An Equality & Diversity assessment form has been completed. ☐

Authorisation	**Name and Position**	**Date Approved**
Responsible Author	Original author IP Weinzweig Updated by A Jones IT Security Co-ordinator	November 2006
Policy Sponsor	Steve Pratt Head of IT Support Services	November 2006

Consideration at authorised groups (e.g. Board, Board sub committees, Policy Group, Clinical policies Sub Group, Departmental meetings etc)

Name of Group	**Minute details**	**Date considered**
Information Governance Committee	Item 10/07	April 2007
IM&T Board		

Executive Summary

This document covers how IT Services controls the storage and access to information held electronically that the Trust uses to support its business including patient data. The field covered is wide and in places technical. The document has been divided into the following sections to ease access and readability:

Introduction; Purposes and aims along with scope of policy

Security Management; Security Roles, Incident Management

Information Security Aspects of Staff Employment: Staff responsibility and accountability

Ownership of and Responsibility for Assets; Ownership of IT assets

Physical Access to IT Equipment, Systems; Building security, maintenance and disposal

System Access Control; Access to Information systems

Security and Confidentiality of Data; Security of Patient data and data backup

Software Protection; Licensing, protection and prevention

System Procurement; Responsible procurement of IT systems

Risk Assessment & Business Continuity Planning Support; Risk assessment, management and disaster recovery planning

Network Security; access to network resources

System Development & maintenance; Information Governance, encryption, security, change control

Compliance; legal requirements and regulation

Appendices; Guidelines, Relevant legislation, system manager functions

1. Introduction

Purpose of a Security policy

The IT Security Policy exists to safeguard electronically processed data, to meet legal requirements and to satisfy obligations to the Trust, clients and staff the IT Service support. It recognises security threats to IT information systems and provides a framework for reducing the likelihood of security incidents.

The viability of information held electronically depends on;

- **Confidentiality**: Ensure that information is accessible only to those authorised to have access.
- **Integrity:** Safeguard the accuracy and completeness of information and processing to ensure confidence in the authenticity of the information.
- **Availability:** Ensure that authorised staff have access to information and associated assets when required.

The IT Security Policy is consistent with and supports the Trust policies and existing methods of working, including Standing Orders, Standing Financial Instructions which take precedence on any specific issue, and is in accordance with NHS national guidance on Information Governance.

The Aims of a Security policy

- All of the Trusts computer systems are secure and confidential. In particular that these are operated in accordance with NHS policy guidelines, ISO 17799 standard, Caldicott Guidance and relevant legislation such as the Data Protection Act (1998). To understand this issue more, refer to the Trusts Information Governance Committee.
- All staff are made aware of this policy, the need to ensure appropriate secure and confidential handling of all personal and business sensitive information and their responsibilities in maintaining information security.
- Confidentiality, integrity and availability are maintained.
- Staff adhere to the principles laid down in the Data Protection Act (1998) and the Caldicott Report.
- Procedures to detect and resolve security breaches are in place.

Where staff believes that it is not possible to meet the policy and associated guidelines this must be brought to the attention of the IT Service and Information Governance Group. Any action agreed to be notified to the appropriate management level within the Trust.

Failure by any staff of the Trust to adhere to the policy and its guidelines will be viewed as a serious matter and may result in disciplinary action under the Trusts Human Resources policies. Please refer to the current HR policies for up-to-date information.

The Scope of the IT Security Policy

The scope of this policy covers the following areas:

- Safeguarding the Trusts electronic records from loss, destruction or falsification.
- Compliance with data protection and other legislation.
- Security Incident reporting and Investigation support.
- Control of the copying of proprietary software.
- Virus and Malware detection and prevention
- Control of access to the *NHSnet (N3)*
- Compliance with the Trusts Information Governance strategy.

For advice on any part of this policy, please do not hesitate to seek advice from the IT Service, who can be contacted via the IT Service Support Desk.

Key References

Ensuring Security and Confidentiality in NHS Organisations

(E5498) Health Service Guidance (HSG1996/18) - The Protection and Use of Patient Information.

2. Security Management

2.1 Introduction

Security is everybody's business and therefore it is everybody's responsibility to ensure information is appropriate, confidential, accurate and available to authorised staff. This section describes the different areas of responsibility and roles within the IT Service that have an affect on the security of information.

The Trust Information Governance Committee shall approve this IT Security Policy as part of compliance with Information Governance (which includes reference to the NHS national mandated ISO17799 standard).

The Head of IT Support Services is responsible for developing, implementing and monitoring the Policy for the IT Service department.

This document will be reviewed annually by the Head of IT Support Services, with input from the IT Operations Manager and other specialities within the IT Service. There will also be an ongoing review of the IT Service policies and operational procedures against this policy and feedback reported to the Head of IT Support Services.

2.2 Security Roles

The responsibility of the various aspects of Information Security is shared between all staff in order to cover the wide physical dispersion of the county sites, including GPs' surgeries. Copies of the relevant IT Security documents are to be made available to each supported NHS organisation and nominated information security personnel, along with publication on the Trust Intranet.

2.2.1 Department Managers

Department Managers as the budget holders are responsible for all computer equipment and peripherals in their department, i.e. visual display units (VDUs), printers, scanners, personal computers (PCs) etc. In detail their responsibilities include:

Equipment:

- Maintenance of a register of all computers in their department/site.
- Physical safety of all computers and peripherals.
- The correct installation of consumables, e.g. printer ribbons, toner cartridges, etc.
- That purchasing of new equipment is made in line with Trusts procurement requirements.
- That appropriate virus checking software is in place.
- Logging and reporting of security incidents.

Staff:

- Ensuring all staff use systems and equipment securely and have training made available for them to do so.
- To enable all staff within their department/site comply with the Trusts Information Governance, IT Security policy and procedures.
- Upon staff termination of employment, departmental property is returned including identity badges, Smartcards and any user rights are removed from IT Service systems.

2.2.2 System Managers

Each centrally resourced software application: (for example; PAS, SMARTSTREAM, SUNRISE CLINICAL MANAGER, CHILD HEALTH, etc.) to be controlled by a named System Manager who shall be registered with the IT Service.

Where System Managers are IT Service staff, they are responsible for the running of the system and for the integrity of the data, i.e. data ownership.

Where System Managers are non IT Services staff, a Data Owner shall be identified and registered.

Responsibilities of System Managers:

- Control of access to the system, i.e. setting up user accounts and allocating access levels and passwords.
- Removing accounts when staff terminate their employment.
- Ensuring the delivery of appropriate user training in both the use of the application and the security aspects of the application.
- Agreeing fixes and upgrades to the system.
- Liaison as appropriate with the IT Service.
- Ensuring system procedures are documented.
- Evaluating operational procedures to identify potential security risk(s).
- Recording and acting upon security violations of the system.
- Ensuring that output from the system is distributed securely.

(Functions with high security risk should be performed by 2 persons to avoid fraud or misappropriation.)

2.2.3 Data Owners

The Data Owner is nominally the organisation for which the system stores data. Day to day management of the data is under the System Manager's responsibility or has been delegated to staff of the owner organisation. Their responsibilities include:

- 'Ownership' of the data, i.e. responsibility for data integrity.
- Liaising with the IT Service regarding system access problems.
- Liaising with the Application System Manager regarding operational procedures.
- Supporting other users of the system.
- Registration of any personal data held under the Data Protection Act 1998.
- The disposal or archiving of data shall be to the relevant Trust Policy (Records Management Strategy) under the control of the Health Records Manager.

2.2.4 IT Service

- The IT Service is responsible for planning and maintaining the local area networks and associated wide area network links.
- The Head of IT Support Service is responsible for ensuring compliance with the IT Security Policy.

2.2.5 Staff

Each member of staff (including those under contract, agency, casual and bank staff), are:

- Accountable for the function they perform and each has a responsibility to ensure compliance with the Trust IT Security Policy and procedures.
- Required to bring to their manager or the nominated Information Governance Committee attention areas of concern regarding information Security.
- Required to abide by the terms of the Data Protection Act (1998) and Caldicott guidance, plus compliance with other relevant legislation.
- Ensure they have familiarity with anti-virus measures and such software is being maintained with regular updates.

2.3 Security Incident Management

In principle, a security incident is any breach or potential breach of information/security, physical or computer related. Damage to the Trust from security incidents can be minimised by monitoring and acting upon such incidents. All staff, contractors/agency, must report any observed or suspected incidents as detailed below.

2.3.1 Reporting of Software Errors

Application Software

Users of application software should report any functional error to the system manager for the application.

PC Software

Users of PCs should report any suspected Virus or other Mal-ware to the IT Support Desk.

Users of PC applications, which are supported by the IT Service, should report any problem with applications to the IT Support Desk for PC support staff to resolve.

Users of PC applications, which are **NOT** supported by the IT Service, may seek advice from the IT Support Desk, but should ensure that a suitable source of assistance is available from the supplier of the application. The applications supported are detailed in the SLA signed up to by the supported organisations to which reference should be made.

2.3.2 Reporting of security weaknesses

Users of the IT Service network should report any observed or suspected security weaknesses to their line manager who will then assess the significance of the incident. The Incident Report Form (IR1) should be completed. Once the line manager has assessed the incident he/she will take appropriate action according to the seriousness of the incident.

Examples of the type of incidents to be dealt with by Line Manager:

- Disclosure of password to another person within the Trust with same system access levels.
- PCs/VDUs left logged in and unattended in secure areas, i.e. not open to the public.
- Printer output not distributed, i.e. left on the printer in secure areas, not open to the public.
- The integrity of the system or data being accidentally put at risk.

Examples of more serious incidents that must be reported to the Data Protection/Risk Manager (or Information Governance Committee):

- Disclosure of confidential information to any unauthorised individual.
- Disclosure of password to another person in or outside the Trust, which could enable unauthorised access to computer systems.
- Attempted unauthorised access to computer systems.

- PCs/VDUs left logged in and unattended in public areas.
- Printer output not distributed, i.e. left in an insecure area and accessible to unauthorised individuals.
- The integrity of the system or data being deliberately put at risk.

3. Information Security Aspects of Staff Employment

Staff must be made aware of their responsibility, accountability and the limits of their authority

3.1 Job structure

Trust management must ensure that, where practical, there is:

- segregation of function and separation of duties
- dual control and staff rotation
- documentation of significant work
- sharing of expertise
- individually defined levels of authority
- restriction of security privileges
- restriction of access rights to specific job functions
- no conflict of interest in job responsibilities

Job definitions

Job descriptions shall include any information security responsibilities that apply to the post, such as the responsibility for:

- implementing or maintaining information securely
- the protection of IT assets
- the information security aspects of processes

Confidentiality agreement

- all staff must sign an appropriate confidentiality Code of Conduct (non-disclosure), which shall form part of their contract of employment
- contract staff must be subject to the same codes of conduct and discipline as permanent staff
- confidentiality agreements must be revisited when terms of employment of individuals change or when employment is terminated

3.2 Staff training

All users of IT (including temporary, voluntary, contract and bank staff) must be briefed on:

- The IT Security Policy for the Trust
- The Data Protection Act (1998)
- The Computer Misuse Act (1990)
- The Copyright, Designs and Patents Act (1988)

- The Access to Health Records Act (1990)

And any relevant acts or directives that come into force after the date of this policy document.

All users of IT Services must be informed of their individual accountability and the disciplinary procedures that may be invoked, should a breach of information security occur.

Job termination or change

Prior to a change of duties or termination of employment, the line manager must ensure that:

- staff is informed in writing that he/she continues to be bound by the signed confidentiality agreement
- computer accounts are removed and the passwords to common accounts are changed
- the staff's name is removed from authorisation and access lists
- staff working out notice are appropriately monitored or assigned to non-sensitive tasks
- departmental property is returned, particular attention being paid to keys, passes, access cards, Smartcards and personal identification devices
- reception staff and others responsible for controlling access to premises are informed of the change or termination, where this is appropriate

3.3 Compliance with statutory legislation

All staff shall comply with all statutory legislation. At the date of this document, statutory legislation includes:

- Copyright, Designs and Patent Act [1988]

All computer software must be licensed, either by purchase of the licence, or by obtaining the written consent of the owner of the software to it's free usage.

Computer software may not be copied without the owner's consent, except for the purpose of creating a backup copy.

- Data Protection Act 1998

All computer systems containing personal data must be registered under the Data Protection Act with the Data Protection Officer.

It is the responsibility of the system owner/manager to ensure that, where applicable, the system is registered and is maintained according to the principles of the Act.

- The Computer Misuse Act [1990]

Computer users may not access systems or modify computer material unless authorised to do so.

Users who 'hack' into systems or gain access by using someone else's password are committing an offence.

3.4 Prevention of or misuse of IT Service facilities

- no-one may access the Trust systems except when this has been formally authorised and documented
- any use of IT Service facilities which is either unauthorised, or not in the business interests of the Trust, shall be regarded as improper use of the facilities and may result in disciplinary action

3.5 New Staff

Before access is given to new Staff, a User account must be set up on the IT system. Staff must complete a Network Use Agreement form. This is available on the Intranet under IT Services.

Departmental Managers should inform the IT Services of the access privileges that the new Staff require.

4. Ownership of and Responsibility for Assets

Each asset associated with an IT system must have a named owner who has defined responsibilities.

4.1 Ownership of Assets

The named owner is responsible for:

- maintaining an inventory of all assets within the area of responsibility
- specifying what, in security terms, the assets can be used for
- determining who can use the assets and what type of access is allowed
- ensuring appropriate security protection for the assets
- ensuring compliance with security controls

4.2 Central IT Equipment

These are the responsibility of the Head of IT Support Services.

They shall be maintained in accordance with suppliers' instructions.

They shall be kept physically safe by means of environmental controls.

4.3 Central IT systems and databases

A central IT system is any networked system available to more than one concurrent user. Each central IT system and its associated data will be the responsibility of a named system manager who must:

- control access to the application
- ensure that users are trained in the use of the application and its security aspects
- take measures to ensure that all data entered into the system are accurate and complete
- maintain documentation pertaining to the system
- record and act upon security violations of the system
- have responsibility for the distribution of output from the system
- manage and account for any controlled stationery used by the system
- ensure that any personal data held in the system is registered under the Data Protection Act 1998.
- be a data custodian for any personal data, with responsibilities as defined in the Data Protection Act 1998.

(System Manager Functions are described in Appendix C)

The physical security of the central IT systems and databases is the responsibility of the Head of IT Support Services who must ensure that:

- the systems and databases are backed up regularly
- copies of the backup media are stored off-site
- procedures are in place to recover systems as soon as possible after a failure

4.4 Computer Peripherals

PCs, VDUs, Printers, light guns, etc:

- are the responsibility of the head of the department at which they are located
- must be kept physically safe against unauthorised use
- must be used with due care, any malfunction being reported to the IT Support desk.

4.5 PC Applications

Applications held on individual PCs or departmental PC networks are the responsibility of the head of the department, who shall have System Manager responsibility as listed in Appendix C and, in addition, must:

- ensure that the application and its data are backed up regularly
- ensure that any personal data held in the application is registered under the Data Protection Act 1998
- permit audits of the PCs and applications

5. Physical Access to IT Equipment, Systems

Resources associated with information processing, such as offices, buildings, computer equipment, electronic services, communications media and paper based records shall be protected from unauthorised access, misuse, damage or theft.

5.1 Building Security

All IT Service facilities that support critical and sensitive business activities must be housed in secure areas. These facilities must be physically protected from unauthorised access, damage and interference.

Rooms shall be lockable and windows secure to break-ins.

In vulnerable areas, the installation of an alarm system must be considered as well as mechanism to physically secure equipment so that it is difficult to remove.

5.1.2 Entry Controls

- Data locked door codes must be given only to named personnel
- Door codes to be routinely changed (recommended annually)
- All staff to have physical identification
- Visitors shall be supervised and required to wear a visible authorisation badge and their date and time of entry/departure recorded

5.2 IT Equipment security, positioning

Guidance on accommodation and operating environment for IT Equipment is provided by the British Standard BS7083 which should be consulted when any questions of suitability arise.

Monitor screens, VDUs and printers, which are located in public areas, must be positioned such that no unauthorised viewing of confidential information can take place.

Where possible all IT Equipment rooms are to be environmentally controlled by the use of air conditioning which is monitored.

Where possible all IT Equipment rooms to be fitted with fire suppressant systems or provided with fire extinguishers.

5.3 IT Equipment maintenance

According to assessed risk, maintenance agreements for all IT equipment shall be taken out.

Where appropriate, maintenance agreements must include a confidentiality clause to ensure information security.

On-going maintenance arrangements must be the subject of contractual agreement, records will be kept of all faults

Only authorised staff shall be allowed to work on IT Equipment, i.e. IT Service staff or authorised contractors. Contractors should be escorted and supervised whilst on site.

5.4 IT Equipment Power Supply

Critical IT Equipment must be protected from power outages, brownouts, power spikes and other electrical anomalies.

Power and telecommunications lines into IT facilities shall be protected against electrical anomalies.

5.5 Security of systems, data, off-premises

- Equipment, data, software or paper records may not be taken off-site without documented management authorisation.
- Portable computers must be protected against damage and theft and not left unattended in any circumstances.
- Media holding software or data must be protected against damage and theft and not left unattended in any circumstances.
- Paper records containing personal and confidential information must be protected against damage and theft and not left unattended in any circumstances.

5.6 Disposal of IT Equipment & Media

5.6.1 IT Equipment

Disposal of IT Equipment shall be managed and not thrown into a skip or sold onto Staff at the end of the equipment's use. IT equipment disposal is an integral part of the auditing process from purchasing of equipment to end of service. IT Equipment has also been classified as Hazardous Waste due to the make-up of the electronic components. Reference the IT procedure ***Disposal of IT Waste*** for the latest information and user guidance.

- any data residing on equipment which is to be disposed must be destroyed before the equipment leaves NHS Trust premises or by the third party contractor with control of standard identified in contract.

- software residing on equipment which is to be disposed must be removed before the equipment leaves NHS Trust premises, unless there is documented agreement between the software supplier and the disposing organisation that the licence will be transferred

5.6.2 Media

The following list identifies typical computer media that requires secure disposal:

- CD/DVD and hard disks
- USB memory sticks, pens and drives
- Magnetic tapes/cartridges used for backups
- Voice & video tapes/cartridges used in surveillance systems

The relevant Trust Policy (Records Management Strategy revised January 2007), is available on the Trust Intranet or via the Head of Information Governance. I must be consulted for the correct retention period and means of disposal.

6. System Access Control

Access to IT Information Systems must be strictly controlled and only allowed on a 'need to know' basis.

6.1 System access

Access to individual applications is controlled by the system manager of the application, who shall:

- assign accounts to users
- assign levels of access to users on a 'need to know' basis
- maintain records of users
- train users in the correct use of the system
- regularly review access controls to ensure that they are still appropriate
- ensure that there is a process for knowing when a user changes jobs or leaves the Trust
- remove user accounts, when a user changes jobs or leaves the Trust
- monitor audit trails

6.2 Password control

Access to systems is further controlled by passwords. Only the person to whom it is issued should use that password. Staff must never divulge a password. They are most effective when they:

- Carry no meaning
- Are not names or have other connections to the user
- Are changed regularly and are not related to previous passwords
- Are a minimum of 8 characters
- Are a mixture of letters, numbers and symbols
- Are kept secret
- Are not the same as the user name or similar
- Are not shared or written down.

6.3 Third party access

When contractors are employed to assist with development or support of the IT Service systems, they **MUST** sign a Confidentiality Agreement (Trust Code of Conduct) before starting work.

Organisations providing remote support must be encouraged to do so over NHSnet(N3) or a secure link using strong authentication such as used by vpn etc.

Third party access to the IT service network must follow the NHS Connecting for Health Code of Connection.

6.4 Third Party

Where development or support is outsourced to a Third Party, due consideration must be given to the NHS policies relative to this situation in the negotiation of any contract. Refer to the Connecting for Health web site for guidance.

Each member of the Third Party's staff involved in the development or support task **MUST** sign a Confidentiality Agreement (Trust Code of Conduct) before working on the project.

7. Security and Confidentiality of Data

Staff working within the NHS have a personal common law duty to their employer and to the patient, to keep information about the patient confidential. This duty continues after staff leave the NHS and also after the death of the patient.

7.1 Introduction

There is routine sharing of information between organisations for general operational activity and also strategic sharing of data for planning and development purposes, which may be both regular and ad-hoc.

The top level document for the sharing of PID is on the Intranet under the Gloucestershire NHS Protocol for Sharing Patient-Identifiable Information between organisations. This is also backed up by the most up-to-date Gloucestershire Hospitals Information Sharing Agreement.

This section outlines the points that need to be considered during day-to-day handling of information that is patient related.

7.2 Confidentiality of patient data

- Discussion about a patient shall be confined to the minimum necessary to do the job effectively
- Disclosure of information, within the Trust, about a patient shall only be done on a 'need to know' basis
- Reading information about a patient, whether on paper or on electronic media, shall be confined to the minimum necessary to do the job effectively
- Storage of the Trust's patient data must be managed and maintained in a secure manner. This applies to any storage media and to any storage location (including premises outside of the Trust)

7.3 Patient data relayed to other organisations

Patient data may be relayed to other organisations directly involved in the provision of care to the patient, provided that:

- the purpose is necessary and fully justified
- access to the data is restricted on a 'need to know' basis
- the use of the data complies with the law
- the receiving organisation has security and confidentiality protocols which are explicit, lawful and monitored

Patient data may be relayed to organisations not involved in the provision of care to the patient, if it is anonymised before leaving the Trust.

Exceptions to this rule are include if:

- the patient's care would be otherwise compromised and the transaction is authorised by the clinician in charge;
- the individual patient gives written informed consent to the transaction;
- the data is required by an authorised body, e.g. the Courts, and is sanctioned by the Caldicott Guardian, Data Protection Officer or Head of Legal Services.

7.4 Methods of Sharing Data

The methods of relaying information about patients must be made as secure as is possible:

Telephone
The identity of the person requesting or receiving the information must be first verified before passing any information.

Facsimile
Any patient data relayed by facsimile must be anonymised as far as is practical, and must be in accordance with the Trust's facsimile protocol.

Verbal
Conversations about patients must take place discreetly and in private.

Electronic
The electronic transmission of patient data will only take place across NHS-net and will also be subject to the network security protocols of the Trust and national encryption standards.

E-Mail
E-Mail generally is not a secure form of transmission and must not be used for the transmission of confidential or sensitive data. However systems and recommendations are constantly changing. To ensure that email is used correctly please refer to the latest information in the document: ***Email Policy***, which is accessible on the Intranet.

Others
Sharing of printouts of patient identifiable data, passing this data to another through the post without marking it confidential, etc.

7.5 Data Storage

Sensitive information must **NOT** be stored on individual drives on PCs. This information is to be stored on the network file servers where available, with access strictly controlled by access permissions.

Should a need arise for local temporary storage, then the IT Support desk must be contacted to approve and instruct on adequate physical security and backup arrangements.

If information is copied between systems on the network, then staff should ensure that any confidential information remains secure and that the recipient system has the same or greater standard of security protection as the first.

7.6 Data Backup

7.6.1 Centrally Hosted Servers, Applications

Data located on central network file servers must be backed up in accordance with written procedures. Such data must be stored securely, off-site as necessary, according to a risk analysis for disaster recovery purposes.

Backups shall be arranged to provide at least one month information retention for critical systems.

All backup media must be maintained securely and erased securely when no longer required.

7.6.2 Local Department or site servers

Data located on departmental or site specific backup servers must be backed up in accordance with written procedures. The responsibility for these data backup systems lies with the Departmental manager or site security person. IT Service will supply technical and support services if requested.

Backups must be stored securely, off-site as necessary, according to a risk analysis for disaster recovery purposes, to facilitate a maximum loss of one calendar week of information destroyed as a result of local building or system damage.

Backups must be arranged to provide at least one month information retention for critical systems.

All backup media to be maintained securely and erased securely when no longer required.

7.6.3 Management of Media

All media containing data, i.e. disks, tapes, CD/DVD-ROMS, etc., containing important data (system, application software, data files, archives) must be stored in a safe secure environment and erased securely when no longer required.

Copies of all licensed software (CD or DVD) must be inventoried to assist in audits and Disaster Recovery procedures.

8. Software Protection

All software used in the Trust must be licensed. The integrity of software and data must be protected, against loss and malicious damage. The introduction of computer viruses on personal PCs is a particular risk, which can be minimised by following good protocols.

8.1 Use and installation of Software – Licensing

Under no circumstances should software, other than that approved and authorised, be loaded onto Trusts computers. Staff must not bring or download software (from the Internet or other computers) onto NHS organisations premises without first getting permission from the IT Service Support Desk. This includes software downloaded from the Internet for shareware and trial or demo purposes.

It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to prosecution.

All changes to and installation of software programs may only be undertaken under the direction of the IT Services Support Desk.

'***Games***' software, except for the purpose of authorised training is not permitted for use on IT Services equipment and must not be installed or used on Trust premises.

Authorised training software includes "***games***" shipped as part of MS Windows.

- All proprietary software must be properly licensed for each machine on which it is loaded. Installation media (CD or DVD) to be stored securely for audit and recovery purposes (such as a re-install).

- Copyright software must not be copied without the owner's documented authority, i.e. each software installation copy needs a licence – either individually or a specified site licence.

- Without infringing copyright, a lawful user of a computer program is allowed to make a back-up copy for disaster recovery purposes only.

- Software installations may be audited at any time by either the IT Services or internal/external auditor. Note; this can now be done remotely across the network. Illegally installed software will be reported to senior management and arrangements made to legally licence or delete.

- Copying of proprietary or Trust software onto computers that do not belong to the Trust is in breach of the information security policy, unless it is for Trust business and authorised by a senior manager. This is still however subject to licensing conditions.

8.2 Procurement of PC application software

- software may only be purchased from suppliers who are approved by NHS Procurement or have recognised quality accreditation

8.3 Installing PC application software

- application software must be installed by the IT Services or by departmental staff approved by the IT Service

- all non-shrink wrapped software must be virus checked and evaluated before installation

8.4 Loading data on PCs

Only data necessary to the business of the Trust may be loaded onto Trust PCs

If the PC does not have virus checking software installed then ALL media containing data must be virus checked before being loaded. This applies even when the media come from:

- another PC in the Trust
- a PC at the user's home
- a PC belonging to a support or maintenance organisation

8.5 Downloading software from the internet

- software must not be directly downloaded from the Internet

- any requirement for software which is available on the Internet should be channelled through the IT Support desk

8.6 Protecting software and data against loss

All software and data must be backed up according to documented procedures.

Backup of Central Systems

The backup of software and data on central systems is documented in the procedures of the IT Services.

Backup of PCs

The procedures for the backup of software and data on PCs will depend upon the usage of the PC and are subject to local risk assessment. The recommendations for backing up to external media such as tapes, USB memory or external hard drives are:

- a monthly backup of the entire machine
- a weekly or daily backup of volatile files

Backups, if made to tape/cassette, should be made on a cycle of at least three, one of which is stored distant from the PC.

PC virus protection and prevention

Viruses and associated malicious software can destroy, lock access to, or pass confidential data to a third party. So to protect IT Services data and systems, all users need to be aware of the need for anti-virus measures.

- All of the Trusts PCs must run updated anti-virus software.
- Users should not use computer media that has not been checked for viruses.
- Users should not send computer media to the outside world without checking for viruses.
- Users must contact the IT Support Desk if a virus incident is suspected.

Clear Screen Policy

Workstations require a username and password to be entered before accessing any software on that PC. Windows screen savers with password protection will be used on all PCs with time out set between 1 & 5 minutes within sensitive locations and a maximum of fifteen minutes at other location.

Personal Use of Trust Systems

All computer equipment leaving the Trust premises should be authorised by the line manager and a copy of the authorisation should be passed to the IT Support Desk.

Removal of Property

Equipment, information or software should not be taken off-site without authorisation from department managers.

Equipment and software will be subject to a process of logging out and back.

Spot checks will be undertaken to detect unauthorised removal of property. Staff will be informed that these will take place, although not when or how.

8.7 Software developed by the Trust

Staff may only develop software, in pursuit of their Trust duties, and with the express permission of the head of the department in which they work.

Any software written by a staff member of the Trust is the property of the Trust, unless there is a contrary agreement which has been documented and approved by the Trust Management Board.

9. System Procurement

Systems must be selected, procured and implemented in a responsible manner with security aspects addressed at all stages.

9.1 Planning and Procurement

The planning and procurement process must ensure that:

- security requirements are addressed and any existing security arrangements are not compromised
- any effect on existing systems, network management and computer operations is evaluated and agreement reached with all affected parties
- account is taken of existing contingency and disaster recovery arrangements and that the effect of adding a new system is evaluated

9.2 System Security Requirements

- The system must include data validation checks, audit trails and internal processing validation
- The system must be allocated a named System Manager, with responsibilities as defined in Appendix C
- The system must be documented, to a level in keeping with the size of the system.

At minimum, the documentation must include the following sections:

- purpose of the system
- name of the System Manager
- security standards that apply
- type of data processed
- number and type of users
- system configuration
- risk assessment and contingency plans

9.3 System Acceptance

Acceptance procedures must ensure that all security standards have been adhered to and tested.

9.4 Standards

The selection, procurement and implementation process must be in line with the following standards:

- as required by legislation
- international, European or National standards
- mandated by the NHS Executive
- Trust standards
- de facto or industry standards

9.5 Standards for Procurement

The procurement process must:

- follow the steps of POISE (Procurement of Information System Effectively)
- address the Private Finance Initiative (PFI)
- include the use of the STEP (Standards Enforcement in Procurement) questionnaire
- be in line with Trust standing financial instructions

9.6 Standards for implementation

The project must be managed according to an approved methodology, such as the NHS standard methodology for Project Management - PRINCE2

9.7 Change control

Changes to systems may only be authorised by the System Manager.

Any effect on existing systems, network management and computer operations must be evaluated and agreement reached with all affected parties

Changes to the system must not alter, degrade or compromise:

- security controls
- access rights
- audit and security software

A record of all changes must be maintained, which includes:

- date and time of change
- details of change
- identity of person/organisation making the change
- any effect on other systems

10. Risk Assessment and Business Continuity Planning Support

The IT Service shall support the Business Continuity processes of the Trust to handle any Disaster incident and Recovery that affects IT Systems. The security of IT systems must be regularly assessed and plans maintained to restore critical business processes in the event of serious interruption as agreed with the Trust Business Continuity teams.

Risk Assessment

All IT systems that have been defined as critical to the business of the Trust must be identified and recorded as such.

Possible threats to the IT Systems must be identified such as;

- Fire, flood, impact damage
- Equipment & component failure, severe capacity restriction
- Power supply withdrawal
- Malicious attacks including physical and network/system intrusion
- Theft/destruction of information and equipment resulting in unavailability, lack of access to information

The impact of an incident resulting in a Disaster being called must be evaluated, together with the likelihood of its occurrence so that a Recovery plan can be prepared and approved.

Risk Management

From the risk assessment;

- the level of risk must be evaluated for each system and appropriate risk reduction measures selected such as additional system resilience
- the risk reduction measures which are selected must be effective and cost efficient
- the risk reduction measures must be documented and approved against the Trust business continuity plan

Disaster Recovery planning

The disaster recovery plan must:

- describe the immediate actions to be taken to recover from an incident
- define responsibilities
- identify alternative service provision and or accommodation
- contain all contact information for involved parties
- specify how staff will be kept informed
- define recovery procedures

Documentation

- the disaster recovery plan must be documented
- the documentation must be regularly reviewed and updated

Testing

- the disaster and recovery plan must be regularly tested at least annually for each identified critical IT system
- the results of the test must be recorded

11. Network Security

The Trust network is controlled by the Infrastructure Manager who is responsible for implementation of appropriate control and security mechanisms to prevent unauthorised access to network services

Responsibility for the Trust network services equipment

The IT Service is responsible for the Trust network and must ensure that the network is:

- designed to include resilience, where possible
- supported and maintained
- protected from unauthorised access
- documented
- monitored for usage

Logging onto the Trust network services equipment

Log-on processes must minimise opportunity for unauthorised access by:

- assigning a unique identifier to each user
- displaying a notice warning against unauthorised access
- limiting the number of unsuccessful log-on attempts
- generate an audit trail of successful and unsuccessful log-on's

Access from non-NHS networks

Access to the Trust network from a non-NHS network must be:

- confirmed as necessary by a System Manager or Head of Department
- subject to strong authentication procedures
- subject to security and confidentiality agreements
- in accordance with the NHS-net (N3) code of connection

Remote diagnostic port protection

Any network services equipment that has a remote diagnostic port must have access control set such that only authenticated access is allowed.

Network routing/connection control

Controls must be in place to ensure that source and destination addresses are correct and reviewed regularly such that the security of information is maintained.

12. System Development & Maintenance

To ensure that information governance controls are built into information systems and processes.

12.1 Information Governance requirements of Systems

Information Governance requirements must be considered in the development of new systems (or extension of existing systems) and processes and include:

Security – Security controls must reflect the business value of the information assets based on risk assessment of failure of a system or access to information for the Trusts.

Confidentiality – The Information Governance lead must be consulted to ensure that compliance with the Data Protection Act (1998) and Common Law duty of confidentiality are paramount concerns of system and process developments, in conjunction with Trust wide compliance endeavours.

Integrity/Quality – In line with compliance with the fourth data protection principle, data quality must be a specific element of system/process analysis and specification.

12.2 Governance in information systems and processes

To prevent loss, modification or misuse of data in electronic information systems. Controls on input, processing and output of data shall be built into IT systems.

12.2.1 Input Data Validation

Electronic data collection processes must have rule based data input designed into them along the following guidelines:

- Value ranges – Acceptable ranges must be built into systems so that only values within the determined range will be accepted.

- Invalid characters – Data collection fields must only accept characters relevant to the data item being collected (e.g. numeric characters must not be allowed in ‘name’ fields).

- Missing or incomplete data – Electronic systems shall feature rules (that may allow local configuration) that indicate to users when required data items have not been completed before data collection screens can be committed (saved to the database).

- Identifiers – The NHS Number ideally should be used as the common identifier on all electronic patient record's or at least be traceable to. The IT systems ideally shall ensure processes around data collection and transfer, capture and use the NHS number. Local identifiers (hospital numbers) are permitted.

Responsibilities for review and development of input/collection validation shall, by default, lie with the System Manager.

Validation routines within data collection shall be part of operational processes required for 'Data Accreditation'.

12.2.2 Control of Internal Processing

Elements of an IT system that run internal processes on data must be specified in developments and tested before system acceptance. (E.g. creating a result from a calculation run on two data fields.) Regular testing must then be run as a series of validation checks. Frequency of such checks shall be based on the importance of the information asset. Checks must be run as part of change control and system acceptance procedures when system developments affect any of the internal processing.

Standard system reports or processes must be checked so that if they have a running order this is maintained.

12.2.3 Data Authentication

Data items in electronic format must be attributable to the User ID recorded in any audit trail relating to the creation, amendment or deletion of data.

12.2.4 Output Data Validation

Despite implementation of controls on both data collection/input and internal system processing, data cannot be entirely relied on without further checks on 'output'. For the purpose of this policy output is defined as follows:

- Regular or ad-hoc reports compiled from summary of information on multiple records. These may be run by users or specific 'Information Analysis staff'.

- Viewing and use of individual records for delivery and management of care.

Information analysis staff shall be responsible for running regular validation checks on reports. Confirmation of the validity shall require input from the system owners. Typically reports must be validated by comparison with other data/reports.

Use of individual records within the delivery and management of care must be checked as part of a regular programme by clinical audit departments.

Staff line managers shall have a default responsibility to ensure their staffs are familiar with processes/procedures around handling data output, especially with regard to interpretation.

12.3 Use of Cryptographic controls (including encryption)

Cryptographic controls are to be used to protect the confidentiality, authenticity or integrity of information where standard controls do not provide adequate protection, such as information exchange over electronic networks.

Encryption

- Use of encryption for electronic transfers of data shall be encouraged.
- 'Web-based' applications which require the transfer of sensitive data (such as e-referrals) shall use at least 128 bit, Secure Socket Layer (SSL) encryption.
- Encryption of databases shall be encouraged.

12.4 Security of System Files

To ensure that IT Projects and support activities are conducted in a secure manner, access to system files shall be controlled.

12.4.1 Control of Operational Software

Where operational software is vendor supplied, the following controls shall be considered and implemented in contractual agreements. If software is developed 'in-house' the same controls shall be applied where possible.

Updates of operational software must only be performed by authorised staff (supplier side), following authorisation from the Trust.

Updates must not be implemented on an operational system until successful testing and user acceptance is obtained.

Audit logs of all updates to test facilities and operational software shall be maintained.

Previous software versions must be retained as a contingency measure.

Tested roll-back procedures shall be in place along with version numbering.

12.4.2 Protection of System Test Data

Many IT systems have test environments to check updates before they are implemented in live systems. These must be subject to the same security procedures and access controls as operational systems, in addition the following shall also be considered:

- Test systems must indicate via continuous display to the user that they are in a test environment.

- Test systems that are 'populated' with a copy of 'live' operational data must have identifying information in the database scrambled via a system routine. This is required as resource to audit access of data on a test system is unlikely to be available and without scrambling, identifiable data could be accessed by users who do not need to know it.

12.4.3 Access control to Program Source Library

To reduce likelihood of corruption (accidental or malicious), program source library access must be strictly controlled. In the case of vendor supplied software this will be in contract with the supplier, however controls are also applicable to 'in-house' developed software:

- Access to source libraries must be only set up for authorised staff

- Program listings shall be held in secure environments

- Audit log of accesses to source library shall be kept

- Old source programs shall be archived with a note of the operational period (times and dates) of the software.

12.5 Change Control Procedures

Changes to IT systems and processes must be evaluated to check they do not compromise the security and integrity of the IT system or operating environment.

All changes to existing IT systems shall be subject to change control procedures that evaluate the potential impact of change on IT system security, data quality and availability elements. Two forms of changes need to be covered:

- In built IT system functions, such as switches for mandatory fields or user definable code lists.

- Vendor controlled changes, where alteration to software code is required, for the addition of new data collection, processing or functionality.

Change requests must be made via an authorisation process controlled by IT system management and system owners. Following receipt of request, analysis of the impact of changes shall be undertaken by IT system management. Significant change proposals that have not originated from the user base shall be tested with users prior to commitment to change.

In these situations, system management and user base must create a set of formal acceptance criteria for each change. System management of IT systems subject to regular change shall compile a set of acceptance criteria.

Where an IT system has a test environment all changes must be carried out there first and evaluated against the acceptance criteria prior to being installed in live systems.

Changes must be scheduled with the user base to ensure minimum disruption to operational business.

System management must ensure any changes to IT system documentation resulting from change shall be put in place.

12.5.1 Technical Review of Operating System changes

When it is necessary to change or update an underlying IT operating system, applications must be reviewed and tested to ensure that integrity has not been compromised. The IT Service (and suppliers) must lead changes to operating systems ensuring relevant departments are bought in and sufficient time is allowed for testing.

12.5.2 Restrictions on Changes to Software

Both in-house and vendor supplied software must be controlled by restricting responsibility to authorise changes to IT system management and system owners. Changes to vendor supplied software must be governed by contractual agreement with the supplier.

12.5.3 Covert Channels and Trojan Code

The IT Service must protect itself from covert channels and Trojan code that allow unauthorised access to information by applying the following controls:

In-house developed software – Application developers must be bound by contract terms of employment and job description responsibilities from inserting covert channels and Trojan code.

Vendor supplied software – Contractual arrangements must ensure that the vendor does not insert covert access channels or Trojan code. Should these be found to be present in any vendor supplied software, contracts will contain appropriate penalty or termination clauses agreed by legal departments.

12.5.4 Outsourced Software Development

The IT Service must define the contractual arrangements to cover the issues raised above.

13. Compliance

13.1 Compliance with legal requirements & regulation framework

To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any IT security requirements.

13.1.1 Intellectual Property Rights (IPR)

The IT Service must comply with legal restrictions on the use of material subject to intellectual property rights such as copyright, design rights and trademarks. The following controls must be used:

- Staff must not load software onto the Trust network and PCs without authorisation (including downloading software from the Internet), which must include a check on the intellectual property rights (licensing) applicable to the software.
- Capacity requirements in terms of licences for multi-user systems must be monitored to ensure that licences are not used inappropriately. Contractual arrangements must ensure easy expansion of licence requirements.
- The IT Service must actively participate in NHS wide application licensing.
- Copies of software must only be made under the authorisation of the IT Service who will check on licensing requirements.

13.1.2 Safeguarding of organisational records

The following forms of organisational record need to be securely retained for statuary or regulatory requirements, including defence against potential civil or criminal action.

- Patient records
- Staff records (employment contracts, staff reviews, etc)
- Financial records (orders, receipts, invoices, etc)
- Public accountability records (board minutes, papers, etc)

The full list of Trust records requiring safeguarding can be found in the Department of Health Records Management – NHS Code of Practice (2006) in conjunction with the Trust Records Management Strategy (revised January 2007) and found on the Intranet.

Many records must be kept for a number of years; therefore the IT Services must ensure that technology change does not make important records inaccessible. This must be either by maintaining relevant technical standards or by the transfer of data at the relevant time to new technology and media.

13.1.3 Prevention of misuse of information processing

The Trust permits limited personal use of IT facilities and systems, these are detailed separately in the Email and Internet Policies. In brief:

Monitoring of activity shall take place, in line with Lawful Business Practice regulations (2000).

Staff shall be made aware that basic monitoring may take place.

Any misuse of facilities shall be dealt with by Management under the HR disciplinary procedures as detailed in the relevant legislation and this policy.

13.1.4 Regulation of cryptographic controls

Cryptographic controls, when implemented, shall be put in place with appropriate reference to the 'Electronic Communications Act 2000' and any subsequent legislation. They shall also be in line with standards such as E-GIF (Electronic Government Interoperability Framework), and NHSnet(N3) policies.

13.2 Reviews of Policy and technical compliance

To ensure compliance of IT systems with Trust information governance policies and standards, regular review of implementation and applicability of the standard shall be carried out.

13.2.1 Compliance with Information Governance Policy

All areas within the Trusts IT Services must be considered for regular review to ensure compliance with information governance policies and standards. These are achieved via a number of ways:

- As part of the IT Service internal/external annual audit cycle
- Via spot-check programme developed and co-ordinated by the Information Governance team with the county Connecting for Health team
- Via annual Department of Health Information Governance audits

The first element is a local process, and the last is a regulatory requirement. Therefore the middle element shall be developed with both the first and last elements in mind, to ensure no repetition of activity.

13.2.2 Technical compliance testing

As part of the Trust audit cycle, the Trust IT Service must include regular checks on technical elements of the IT infrastructure, many of which are related to security. These shall be required to meet appropriate E-GIF and NHSnet(N3) security/operational standards as a minimum.

13.3 System Audit considerations

The objective is to maximise the effectiveness of and to minimise interference to/from the system audit process.

13.3.1 System Audit Controls

Any required/planned audit must take account of risk to business operations and be planned around required timing. Factors to be included are the removal of key staff to meet with auditors, the scope of checks and the requirement for production of audit reports from the system.

13.3.2 Access to system audit controls

Access to any software tools or reports that form part of an audit system must be restricted to specific individuals.

Appendix A

Short guidelines as to what to do

- Management of Security and the Reporting of Security Incidents
- Security Aspects of Staff Employment
- Software Protection
- System Procurement

Management of Security and the Reporting of Security Incidents

REPORTING SECURITY INCIDENTS	
Person(s)/Purpose	**Action**
1. User	1. Notify your immediate line manager that a security incident has occurred 2. Inform the Information Security Officer, Caldicott Guardian or Data Protection Officer, Risk manager, or Human Resources Information Governance lead, giving full details of the incident. Note: This must be done immediately, by you. 3. If any of the above Officers is implicated in the incident, report the matter directly to the Director of Finance, Information and Computing 4. Discontinue any activity which will make the security breach worse.
2. Information Security Officer	1. Log the incident, according to the guidelines issued by the NHS Executive 2. Investigate the incident and record the outcome 3. Notify the user and the line manager of the outcome

Note: 'User' means the person who became aware of the security breach

Security Aspects of Staff Employment

STARTING EMPLOYMENT	
Person(s)/Purpose	**Action**
Human Resources Dept.	1. Provide new staff with summaries of the following legislation/regulations: • The I T Security Policy for the Trust • The Data Protection Act (1984) • The Computer Misuse Act (1990) • The Copyright, Designs & Patents Act (1988) • The Access to Health Records Act (1990) 2. Ensure that a confidentiality agreement is signed. 3. Include briefing on security of information in the induction day. 4. Inform new staff of disciplinary procedures that may apply if security procedures are not followed.
Line Manager	1. Inform new staff of the security responsibilities that apply to the post. 2. Inform new staff of any other legislation/regulations that are relevant to their post. 3. Arrange any further training which is relevant to the post.

CHANGE OF EMPLOYMENT	
Person(s)/Purpose	**Action**
1. 'Old' Line Manager	1. Remove all access rights that are not relevant to the staff's new post 2. Change physical access codes, if appropriate. 3. Remove staff's name from authorisation and access lists which are not relevant to staff's new post. 4. Ensure either that all departmental property is returned or that the 'new' Line Manager is informed of the items being retained by the staff.
2. 'New' Line Manager	1. Inform staff of the security responsibilities that apply to the new post. 2. Inform staff that confidentiality agreement still applies. 3. Inform staff of any legislation/regulations that are relevant to the new post 4. Arrange any training which is relevant to the new post.

LEAVING EMPLOYMENT	
Person(s)/Purpose	**Action**
1. Line Manager	1. Inform leaver, in writing, that they must still abide by the confidentiality agreement after leaving the Trust's employment 2. Remove all computer accounts. 3. Change any passwords to common accounts 4. Change physical access codes. 5. Remove leaver's name from all authorisation and access lists. 6. Ensure the return of all departmental property.

Software Protection

ACTION ON DETECTING A COMPUTER VIRUS	
Person(s)/Purpose	**Action**
1. User	1. Switch off the PC immediately 2. Notify the IT Services Department on the Help Desk number 08454 222808 3. Ensure that the latest backup is available, in case it is required 4. Report the virus as a security incident (See procedure 2.3)
2. IT Services Department	1. Isolate the machine and remove to the IT Services Department for treatment 2. Virus check any other machines that might be infected

System Procurement

PLANNING AND PROCUREMENT	
Person(s)/Purpose	**Action**
1. Procurer	1. Establish that system is operationally necessary 2. Determine the benefits 3. Determine the effects upon the working practices of the department 4. Evaluate available systems 5. Prepare a proposal or business case for the Project Group
2. Project Group	1 .Evaluate how the proposal fits in with the strategy of the Trust 2. Recommend any necessary technical changes 3. Approve the proposal (if the cost is within approved limits) or reject the proposal
3. Board	1. Approve/reject the proposal (if the cost is greater than approval limits)

If the proposal is accepted:

4. Procurer	1. Commence procurement process, following POISE guidelines and STEP questionnaire 2. Select system
5. Implementer	1. Implement system, following PRINCE2 guidelines 2. Realise benefits

Appendix B

Synopsis of Relevant Legislation

Data Protection Act 1998 (updated)

The Data Protection Act is concerned with the structured filing and/or automatic processing of personal data that is data about living and identifiable people which is either processed by computer or stored in a manual filing system.

Personal data which is held in this manner must be registered with the Information Commissioner via the Data Controller. The registration gives the data user's name and address together with broad descriptions of:

- the personal data held
- the purposes for which it is used
- the sources from which the information may be obtained
- the people to whom the information may be disclosed, i.e. shown or passed on to
- any overseas countries or territories to which the data may be transferred.

Once the data is registered, users of the data must comply with the principles of good practice contained within the Act, which are that the information must be:

- obtained and processed fairly and lawfully
- held and used only for the lawful purposes described in the data user's register entry
- disclosed only to those people, described in the register entry
- adequate, relevant and not excessive in relation to the purpose for which they are held
- accurate and, where necessary, kept up-to-date
- held no longer than is necessary for the registered purpose
- accessible to the individual concerned who, where appropriate, has the right to have information about themselves corrected or erased
- surrounded by proper security.

It is a criminal offence not to register personal data which is held on computer or in a structured manual filing system. It is also a criminal offence to obtain, access or use the data outside the descriptions contained in the register entries.

Contravention of the Act may result in disciplinary proceedings and even legal proceedings.

Access to records of 'live' individuals is processed under the Data Protection Act 1998. Access requests are dealt via the office of the Head of Legal Services.

A copy of the Act is available for inspection in the Data Protection Officer's office at Cheltenham General Hospital or can be found on the Intranet on the Information Commissioner's web site http://www.ico.gov.uk/

Computer Misuse Act 1990

This Act makes provision for security computer material against unauthorised access or modification; and for connected purposes.

It is an offence to:

- Knowingly secure unauthorised access to any program or any data held in any computer.
- Knowingly cause a computer to perform any function with intent to secure unauthorised access to any program or any data held in any computer.
- Facilitate the commission of the offences described above, either by oneself or any other person.

Unauthorised access occurs if the person concerned neither has consent to access nor entitlement to control access.

Program or data includes material held on removable storage media.

It is also an offence to:

- Cause an unauthorised modification, either temporary or permanent, on the contents of any computer whilst having the requisite intent and requisite knowledge.

Requisite intent is the intent to cause a modification which:

i) impairs the operation of any computer or any program
ii) prevents access to any program or data
iii)compromises the reliability of any data

Requisite knowledge is the knowledge that the modification is unauthorised.

Modification takes place if:

i) any program or data is altered
ii) any program or data is erased
iii) any program or data is added to the existing contents
Contravention of the Act may result in disciplinary proceeding and even legal proceeding.

A copy of the Act is available for inspection in the Post Graduate Library.

Access to Health Records Act 1990

The Act gives individuals the right of access, to records of deceased patients, and further details can be obtained from the Head of Legal Services or the Trust Data Protection Officer.

Copyright, designs & Patents Act 1988

Copyright is an automatic property right which authors have in relation to the works which they create. Anybody who creates something is entitled to own it and to be rewarded for their creative endeavour, but their rights are more limited than those normally associated with property. The reason for the limitation is one of the principles contained in the Universal Declaration of Human Rights which states that “everyone has the right freely to participate in the cultural life of the community”. Copyright law balances the interests of the creator and the needs of users to have access to their work.

Copyright is concerned with the intellectual rights of the creative work, as opposed to the ownership of the material upon which the work is recorded, and addresses issues such as copying, adapting, broadcasting and performing the work.

Computer programs are regarded as literary works and come within the scope of the Act. The purchaser of any computer program or application has only purchased the ‘right to use’ the program and may not copy, change or distribute it without the permission of the owner. The purchaser does not own the program but only the media, CD or disk upon which the program was delivered.

It is recommended procedure to back up computer programs and there is an implied licence within the Act for this to be done, although there is no express statutory right.

It is an offence to possess or distribute software for which you do not have a licence, or to collude in such acts. Unfortunately, the Internet provides the means to easily obtain infringing software and to circumvent licensing rules but these actions are still illegal. Copyright law is enforced by Trading Standards Officers, the Police and various organisations such as FAST and FACT.

Staff in the Trust must ensure that:

- Any computer program installed on their PC is correctly purchased and licensed.
- Computer programs are not copied, amended or otherwise distributed (except for backup copies).

Contravention of the Act may result in disciplinary procedure and even legal proceedings.

A copy of the Act is available for inspection in the Post Graduate Library.

Appendix C

System Manager Functions

System Managers are not necessarily accountable for the direct management of staff operating the system and their scope is not constrained by organisational boundaries. In general, their responsibilities cover:

Access Control

- setting up new user accounts
- deleting accounts when staff leave or change jobs
- ensuring appropriate levels of access
- acting as a focal point for breaches of security

Policies and procedures

To develop policies and procedures for the use of the system, including business continuity plans and manual procedures in case of severe system malfunction.

Training

- training of new users
- re-training users following changes to the system
- assisting users to fully develop their use of the system

Documentation

To develop, maintain and issue:

- the User manual
- training material
- operational procedures

Data Validation

To put in place measures that ensure that data entered into the system is accurate and complete, e.g. random checks, cross checks with other systems where possible.

System reports

To be responsible for the distribution of printed output from the system, and to manage and account for any controlled stationery used by the system.

Data Protection

To be custodian of the data in the system, as required by the Data Protection Act, and to ensure that use of the system conforms to the principles of the Act.

Monitoring

To monitor use of the system for adherence to documented procedures and to ensure that benefits are realised.

Communication

To act as a focal point for issues concerning the system:

- to chair the local User Group
- to liaise with technical support organisations
- to promote awareness of the system
- to establish and communicate changes and developments